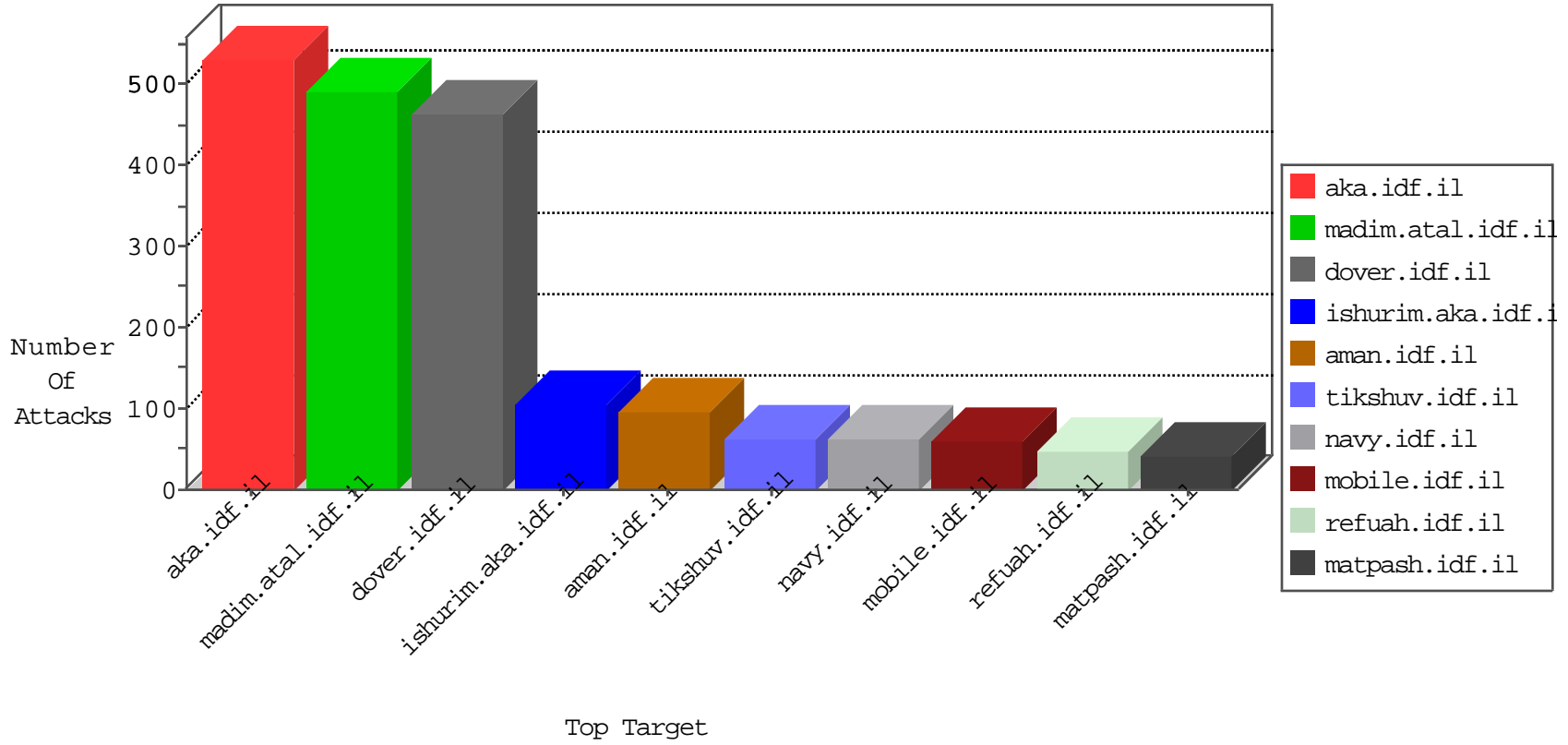


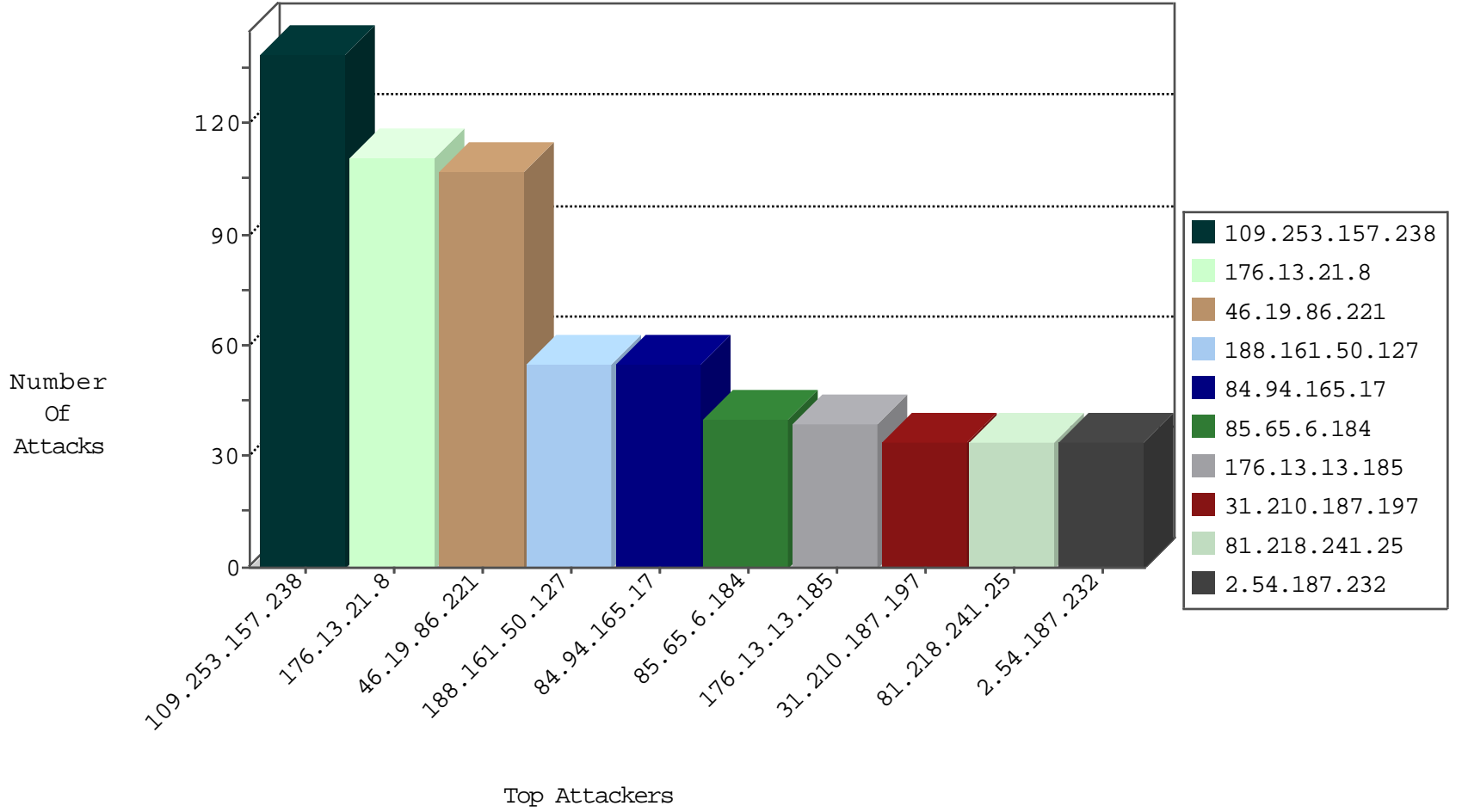
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
185.32.179.217	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
46.19.86.63	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
192.0.100.226	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
173.252.112.102	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
159.104.163.17	United Kingdom	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
23.239.64.15	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
159.104.163.20	United Kingdom	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
101.111.249.164	Japan	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
79.181.189.27	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
141.212.122.204	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.128	Italy	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
5.189.176.187	147.237.77.234	Germany	halag.idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
108.4.143.45	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
89.138.124.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.68.29.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
68.180.228.112	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.173.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.240.213.93	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
180.150.177.188	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.209.61.98	147.237.77.216	Romania	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.195.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.134.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.165.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
207.232.46.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
195.202.72.106	147.237.77.216	Kenya	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.0.236.123	147.237.76.196	Moldova, Republic of	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.21.8	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
109.253.147.220	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
31.210.187.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
85.65.6.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
212.150.245.250	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
188.161.50.127	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	18
176.13.21.8	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
85.65.6.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
79.176.4.236	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
188.161.50.127	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.65.251	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
171.25.193.132	Sweden	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
109.65.0.145	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
171.25.193.132	Sweden	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
87.68.58.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
31.13.113.69	Ireland	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
31.210.187.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
31.154.18.65	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
212.150.245.250	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
194.56.215.218	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
5.28.173.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
37.26.149.175	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.226	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.54.29.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
5.28.173.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.176.135.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.1.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
212.179.243.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
80.246.130.141	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
31.154.18.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
94.230.86.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
81.218.241.25	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
2.54.29.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
81.89.0.199	Romania	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
199.203.226.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.188.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
62.219.183.202	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.110.33	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.150.143.132	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.7	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.45.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
94.230.86.108	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.7	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.187.188	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.149.245	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.157.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	139
46.19.86.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	101
176.13.21.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
84.94.165.17	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 84.94.165.17	Block	53
176.13.13.185	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	30
2.54.25.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.85.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
2.54.187.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
176.228.130.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
2.54.187.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
46.19.86.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
194.90.240.21	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	4
2.54.42.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
217.165.93.177	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
77.125.13.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
2.54.145.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
194.90.240.21	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 194.90.240.21	Block	3
109.253.193.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.17.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.229.157.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.131.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.65.6.184	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.13.185	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	2
46.19.86.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.29.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.0.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.176.10.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.253.130.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
95.86.118.245	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus/&sa=u&ved=0ahukewjbsbj4o8zkahugxq8khepwat0qfggumae&usg=afqjcnhcvyvg7wlcq-yhd5_ammzoyodtwa	Block	2
46.19.85.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
74.82.47.2	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
207.46.13.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1116-he/ÃfÆ'Ãçâ,-âe?ÃfâešÃçÂ ÃfÆ'Ãçâ,-âe?ÃfÃçâešÃ-ÃçÂ?	Block	1
157.55.39.141	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/eng	Block	1
182.59.212.89	India	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.94.165.17	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
176.13.13.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.154.94.46	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Abnormally Long Request method	Block	1
79.177.160.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.18.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.132.242	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout2.css	Block	1
198.20.69.74	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
37.142.64.16	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	1
169.253.194.1	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
80.178.120.40	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
207.46.13.49	United States	147.237.72.166	aka.idf.il	Unknown Parameter 177afae0 in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Abnormally Long Request method	Block	1